IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 4, April 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

9940 572 462 | 6381 907 438 | ijircce@gmail.com | www.ijircce.com

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104211 |

A Multilayered Lightweight and High-Speed Image Encryption Technique based on Hybrid Chaotic Map, Steganography, and Enhanced AES

[1]Shakuntala Bindiya and [2]Vivek Kumar Sinha

[1]M. Tech Student, Dept. of CSE, Raipur Institute of Technology, Raipur, Chhattisgarh, India

[2]Assistant Professor, Dept. of CSE, Raipur Institute of Technology, Raipur, Chhattisgarh, India

ABSTRACT: Throughout the era of technological advancement in communication, secured picture transfer has become one of the biggest difficult issues to solve. On the internet, plenty of individuals utilize as well as share photographs for both private as well as professional reasons. Encryption methods that transform the real picture into an unintelligible or jumbled shape, known as a cipher picture, are one approach to providing secured picture transfer over the web. In the last decade, there have been discussed varied methods for image encryption, however, these methods have some drawbacks such as less security, high complexity in implementations, and low speed. Hence, there is a need to build novel advanced, and high-speed image encryption methods for improved image security. In this article, a multilayered lightweight and high-speed image encryption technique based on the hybrid chaotic map, steganography, and enhanced AES has been proposed. The key outcomes of the proposed research are found very optimized and enhanced.

KEYWORDS: Chaotic Map, Enhanced AES, Image Encryption, Steganography.

I. INTRODUCTION

Digital image encryption has been recognized as a crucial security measure that might assist in maintaining the confidentiality and authenticity of important information. Anytime digital images are transferred over the internet or stored on a device, there runs the risk of being intercepted and accessed without authorization [1], [2]. Encryption could assist in limiting unauthorized access to similar photos since it makes data indecipherable without the proper decryption key. Information alteration or modification may be prevented with the use of digital image cryptography. Any effort to modify confidential data will result in the decoding process failing, letting the recipient realize the data had been changed [3].

Images typically involve sensitive personal information, such as clinical information, savings user accounts, or official documents from a variety of industries, such as the acceptable, financial, as well as healthcare sectors [4]. Encrypting certain images could improve their privacy and secrecy. Electronic image encryption provides a crucial security measure that could help to protect sensitive information and prevent unauthorized access to it [5]. The several forms of encryptions are shown in Figure 1.

The advancement of technological connectivity has made online picture-sharing more convenient. However, if the photographs are exchanged over unsafe channels, their identity could come in danger from specialized attacks. Picture encryption provides one pragmatic method for protecting against the threat to privacy. The bulk of contemporary interaction methods, including messaging, social networking sites, and e-mail, all depend on images to deliver information [6]. However, interacting through unsecured ways increases the likelihood that the photos and other details would be exposed to scammers or unauthorized users. Thus, data or photographs should be protected from intruders to stop potential electronic assaults. The only people who should have exposure to the photos are the sender and receiver. Encrypting photo transmissions sent over the internet has emerged as the most widely used solution to the issue [7].

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104211 |

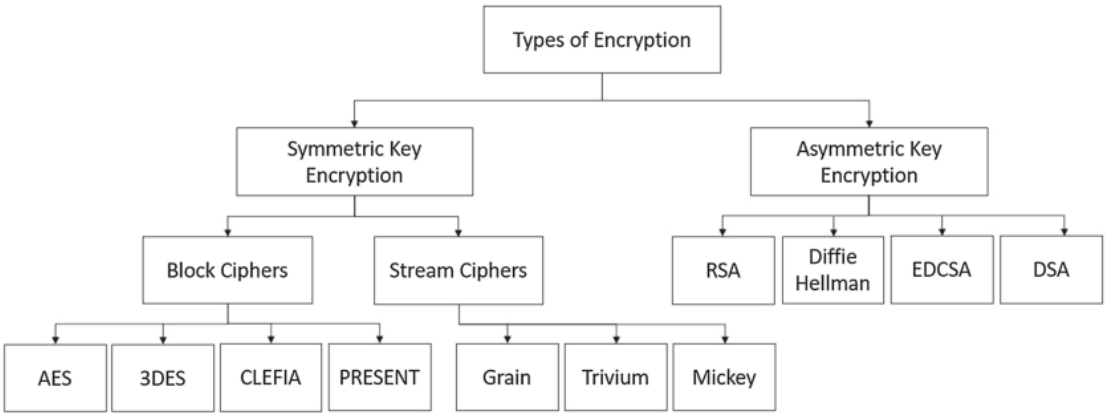


Figure 1: Illustrates the types of encryption[4].

II. RELATED WORK

Owing to its ease of use, affordability, alongside accessibility, the World Wide Web has increasingly impacted the lives of individuals in the past few decades. The Internet has replaced other ways of data transmission as the primary method. In modern times, the World Wide Web has been used to transfer an extensive amount of electronic information. Semi-structured, unorganized, or organized information can all be discovered within this dataset. Data safety is crucial in today's technologically advanced environment [8]. Many businesses and agencies spend a lot of cash securing business assets, notably the confidentiality of the company's workers, and their internet-based transactions, including any sensitive data that is kept or sent in the shape of footage, words, sounds, or images. A technique for protecting electronic photos called transform domain cryptography encrypts the picture after it has been transformed between the spatial realm to another realm, which means the frequency domain or the wavelet domain [9].

This approach aims to increase the integrity of the encoded picture by making use of the distinctive qualities of several transformation realms. This recently proved evident how all public network information transmissions are vulnerable to hostile assaults and therefore might be the subject of a breach. Numerous encryption methods have been proposed only for the protection of telecommunications in particular [10]. This has focused on dynamical cryptosystems which convert plain information into unreadable cipher information, which creates disorder networks. The Data Encryption Standard (DES), Advanced Encryption Standard (AES), as well as Blow Fish (BF), are only a few examples of the various cryptographic techniques that have been created and developed. Such techniques carry out the encrypting as well as decoding stages using a given-length Private Code (PC), given-length block size, as well a given number of rounds [11], [12].

Each of such techniques depends on encryption standards which offer high-grade settings, but they are slow as well as may only be utilized to encrypt or decrypt small-sized information, like written files as well as communications [13]. Conventional encryption techniques for ordinary information are typically not appropriate for picture cryptography because of the large amount of information as well as the significant correlations of pictures. In the past few years, chaotic-based systems have become used extensively in picture cryptography due to their ergodicity, and synchronization, including great responsiveness to model variables and beginning settings. Permutation, which modifies color placements, and diffusion, which modifies pixel values, are the 2 basic processes in picture cryptography [14], [15].

III. PROPOSED METHODOLOGY

In this research paper, a novel multilayered lightweight and high-speed image encryption technique based on the hybrid chaotic map, steganography, and enhanced AES is proposed. The security of the images is becoming a very common issue in this modern era. The previously developed image secrecy approaches have some common deficiencies which include less security of the data, lower speed as well as more complexity in implementation.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104211 |

3.1. Design

The daily utilization of technology, particularly social media sites, web-based surfing, and messaging has grown considerably during the last decade. As a component of the information rupture, multimedia has been distributed by thousands of individuals along with devices that can use connectivity. This growing movement of digital media presents major preservation as well as security threats owing to the growth in hacking incidents in previous years, that involve changing as well as disclosing information obtained via content.

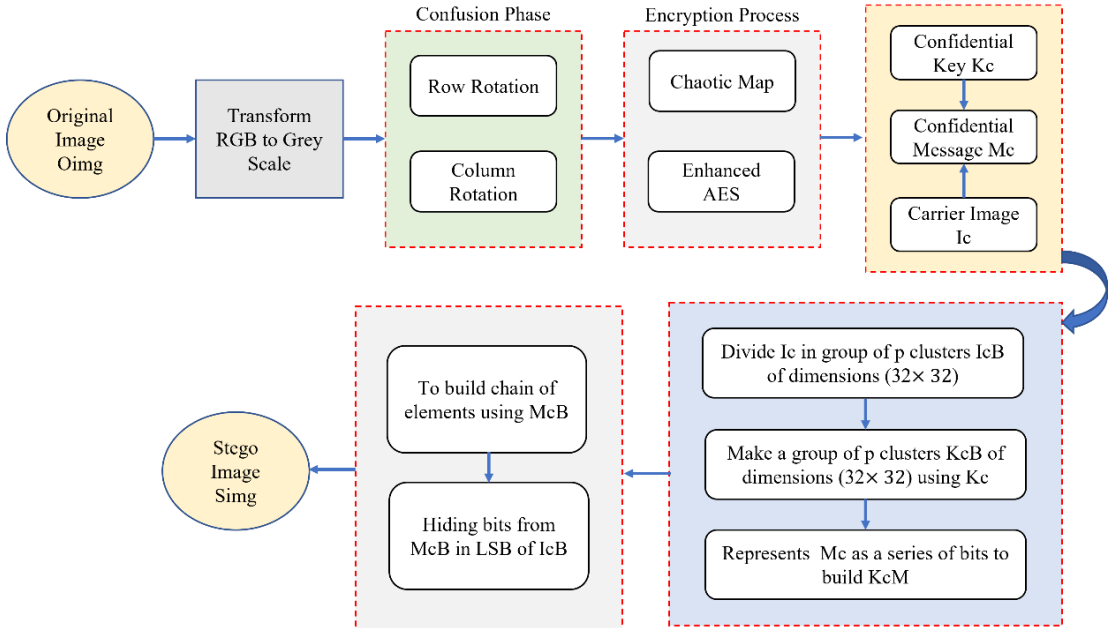


Figure 2: Illustrates the proposed encryption and hiding process.

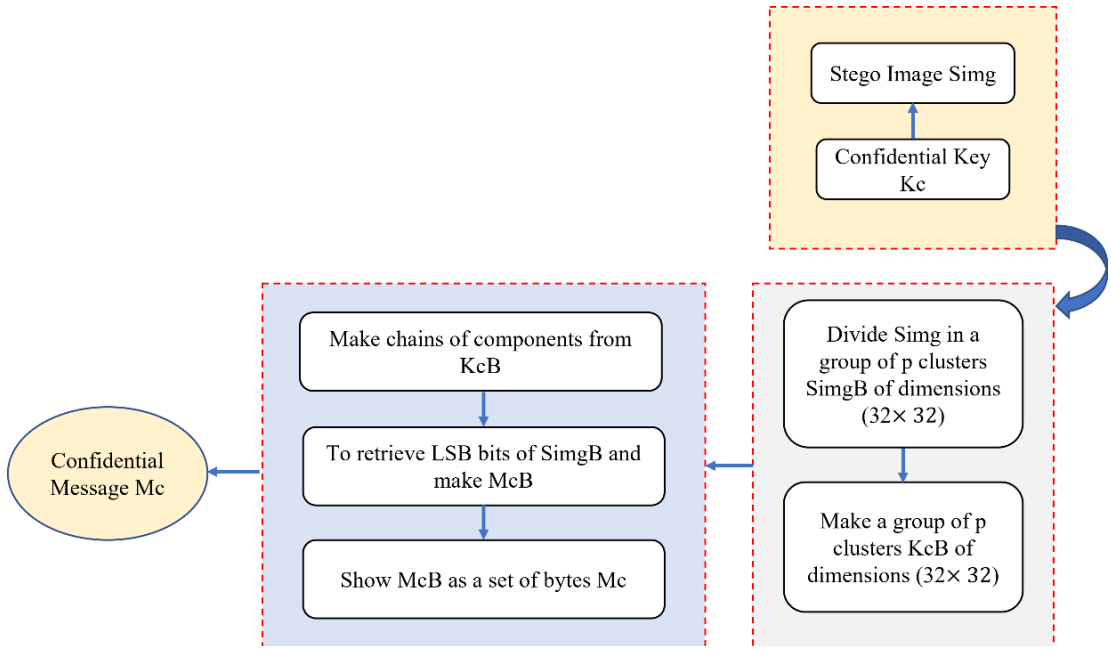


Figure 3: Illustrates the proposed extraction procedure for confidential Message Mc.

Figure 2 illustrates the proposed encryption and hiding process. The working process of the proposed image encryption and data security method is described as follows. In the first step, the original image Oimg is transformed

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104211 |

RGB to the Greyscale. In the next phase for high data security, the confusion phase is performed utilizing the row rotation and column rotation in real-time. In the subsequent phase, the encryption procedure is done using the chaotic map and enhanced AES algorithm. For the steganography operation, the confidential Key Kc and carrier image Ic are combined and used with the confidential message Mc. Furthermore, the preparation procedure is performed and the steps are given as follows.

Step 1: Divide Ic in a group of p clusters IcB of dimensions (32×32).
Step 2: Make a group of p clusters KcB of dimensions (32×32) using Kc.
Step 3: Represent Mc as a series of bits to build KcM.
Furthermore, the hiding procedure is done using the distinct steps which are described as follows:
Step 4: To build a chain of elements using McB
Step 5: Hiding bits from McB in LSB of IcB
Finally, after performing the hiding procedure, we obtained the Stego image i.e., Simg.

Figure 3 illustrates the proposed extraction procedure for confidential Message Mc. In this method, initially, a confidential key that is Kc has been used along with the Stego image Simg for performing the extraction procedure. The preparation steps are described as follows:
Step 1: Divide Simg in a group of p clusters SimgB of dimensions (32×32).
Step 2: Make a group of p clusters KcB of dimensions (32×32)
Furthermore, the extracting procedure is discussed as follows:
Step 3: Make chains of components from KcB
Step 4: To retrieve LSB bits of SimgB and make McB
Step 5: Show McB as a set of bytes Mc

3.2. System Configuration

This investigational analysis for secured image encryption has been conducted on a personal computer (PC) which is installed with MATLAB R2022b. This selected PC involves the described configuration i.e., RAM: 16GB, Windows 11 platform, integrated operating system of 64-bits, and Storage medium: 512GB. The MATLAB software package is one of the most powerful and pragmatic platforms for highly complex image-processing tasks.

3.3. Data Collection

Image confidentiality has become a critical concern since many digital remedies, such as amusement infrastructure, medical interactions, as well as internet-rooted connections, require reliable security for the storage as well as distribution of digital photographs. Considering the growth of internet and mobile interactions, a reliable connection is additionally required. A computerized system like that mayn't in any way compromise the final user's anonymity. To accomplish it, it is essential to maintain data integrity while submitting the original image descriptors. In the present empirical correlation investigation, 3250 randomly selected pairs of neighboring pixels were selected in the real-time encryption as well as unencrypted images across the diagonal, vertical, along with horizontal directions.Table 1 illustrates the correlation analysis used in the proposed method of adjacent pixel evaluation for Pepper, Baboon, Lena, and the cameramen.

Table 1: Illustrates the correlation analysis used in the proposed method of adjacent pixel evaluation for Pepper, Baboon, Lena, and the cameramen.

S.N.	Direction(s)	Horizontal	Vertical	Diagonal
1	Pepper Plain-picture	0.9578	0.9435	0.9177
2	Pepper Cipher-picture	-0.0089	0.0029	0.0085
3	Baboon Plain-picture	0.8988	0.8963	0.9173
4	Baboon Cipher-picture	0.0369	-0.0532	0.9354
5	Lena Plain-picture	-0.0245	-0.0144	-0.0055

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104211 |

6	Lena Cipher-picture	0.0889	0.4588	0.0458
7	Cameraman Plain-picture	0.0335	0.8523	0.1145
8	Cameraman Cipher-picture	-0.0215	-0.0456	-0.2136

3.4. Data Analysis

This experimental research analysis for image encryption and data security, the correlation analysis of the adjacent pixels has been performed using the following mathematic equations. The correlation analysis is a way that relates to the evaluation of two diverse variables along with a unique correlation such as to determine the degree of the correlation of two distinct variables. The image adjacent pixel correlation may reflect image pixels scrambling.

$$E(x) = \frac{1}{N}\sum_{k=1}^{N} x_k \quad (1)$$

$$D(x) = \frac{1}{N} N \sum_{k=1}^{N} (x_k - E(x))^2 \quad (2)$$

$$cov(x,y) = \frac{1}{N}\sum_{k=1}^{N} (x_k - E(x))\,(y_k - E(y)) \quad (3)$$

$$\rho_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (4)$$

Herein the terms x_k as well as y_k illustrates the obtained grey values of the distinct two adjoining pixels.

IV. RESULTS AND DISCUSSION

Overall histograms of the cipher as well as real pictures display greater variance, which eventually reduces the odds of giving the invaders a hint as well as deterring them from assaulting, making AES approach superior behavior within the histogram-based examination of the picture. In contrast to AES, a hybrid chaotic map showed comparable plots for encryption as well as decryption pictures. This indicates that there are fewer variances as well as greater opportunities for attackers to forecast the features of the encoded versus unencrypted photographs. Asa result, it is clear from the research preceding how the composite chaos mapping is more resilient to varied assaults. In comparison to the other previous approaches, the proposed hybrid model based on AES and the hybrid chaotic map is computationally fast since it retains encrypting along with decryption times. AES has the advantage of having a pragmatic PSNR value versus noticeable variations among the histograms of the actual picture as well as the cipher, which helps it retain the picture's features following decoding. The performance outcome of the proposed multilayered lightweight and high-speed image encryption technique based on the hybrid chaotic map, steganography, and enhanced AES has been received more improvement in comparison to previous image encryption and decryption methods. The NPCR and UACI has been found optimized. The evaluation is done in terms of the NPCR, UACI.

$$NPCR = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} DIF(i,j) \times 100\% \quad (5)$$

$$UACI = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|C_2(i,j) - C_1(i,j)|}{255} \times 100\% \quad (6)$$

$$DIF(i,j) = \begin{cases} 0, & C_2(i,j) = C_1(i,j) \\ 1 & C_2(i,j) \neq C_1(i,j) \end{cases} \quad (7)$$

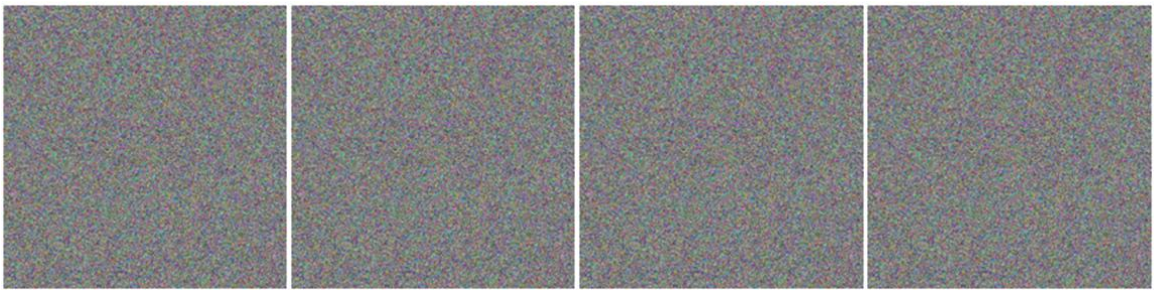
(a) (b) (c) (d)

Figure 4: Original images (a) depict pepper, (b) show Baboon, (c) shows Lena, and, (d) illustrate the cameraman.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104211 |



(a) (b) (c) (d)

Figure 5: Encrypted original images (a) depicts pepper, (b) show Baboon, (c) shows Lena, and, (d) illustrate the cameraman.

(a) (b) (c) (d)

Figure 6: Original decrypted images (a) depict pepper, (b) shows Baboon, (c) shows Lena, and, (d) illustrates the cameraman.

Figure 4 illustrates original images (a) depicting pepper, (b) showing Baboon, (c) showing Lena, and, (d) illustrating the cameraman. Figure 5 shows the encrypted original images (a) depicts pepper, (b) shows Baboon, (c) shows Lena, and, (d) illustrates the cameraman. Figure 6 shows original decrypted images (a) depicts pepper, (b) shows Baboon, (c) shows Lena, and, (d) illustrates the cameraman.

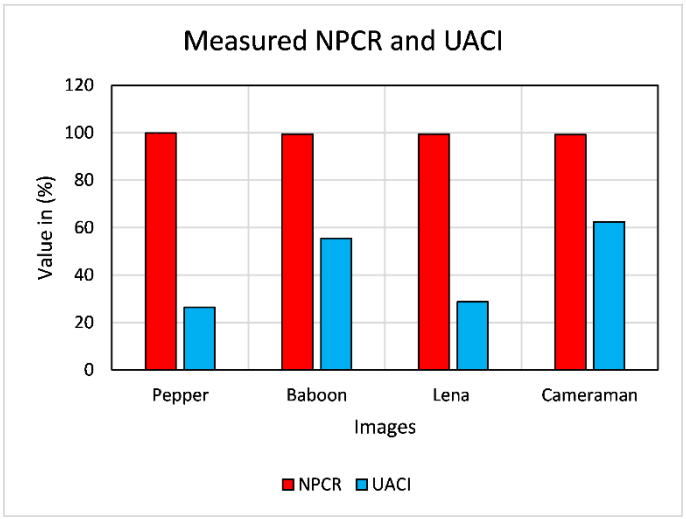


Figure 7: Illustrates the Measured NPCR and UACI.

Table 2 illustrates the time comparison in the encryption process. The existing and our method i.e., Y. Dong et al. [16], Ruifeng Han [3], and proposed method for an image size of 90×90, 128×128 and 256×256 consumes encryption time 2.13s, 0.15s, and 0.9s, respectively. Figure 7 illustrates the Measured NPCR and UACI. For our method, on the images Pepper, Baboon, Lena, and Cameraman the measured NPCR as well as UACI are 99.85, 99.47, 99.4, and 99.19, as well as 26.41, 55.44, 28.66, and 62.36, respectively. All the measured values have been found good and enhanced.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104211 |

Table 2: Illustrates the time comparison in the encryption process.

S.N.	Methods	Size of Image	Encryption time(s)
1	Y. Dong et al. [16]	90 × 90	2.13
2	Ruifeng Han [17]	128 × 128	0.15
3	Proposed method	256×256	0.9

V. CONCLUSION

Throughout this study, researchers suggested three methods for safe picture encryption: Chaotic Map, Steganography, and Enhanced AES. These methods' efficacy for picture encoding was evaluated using a variety of criteria, including unified average changing intensity (UACI), peak signals-to-noise-ratio (PSNR), numbers-of-pixels-change-rate (NPCR), histogram evaluation, including processing time assessment. The findings show that while AES is operationally inefficient, its higher histogram variances, as well as its minimized PSNR number, allow it to keep picture characteristics following encryption. While it appears to maintain fewer picture attributes, the hybrid chaotic technique exhibits elevated NPCR as well as UACI values that demonstrate its power in repelling asymmetrical assaults. Comparing the proposed technique to the other couple of methods, it is operationally fast. Overall study especially findings from the discourse above lead to the conclusion that Chaotic Map, Steganography, and Enhanced AES techniques have a good influence on picture encryption.

REFERENCES

[1] Y. Pourasad, R. Ranjbarzadeh, and A. Mardani, "A new algorithm for digital image encryption based on chaos theory," *Entropy*, 2021, doi: 10.3390/e23030341.

[2] B. Zolfaghari and T. Koshiba, "Chaotic Image Encryption: State-of-the-Art, Ecosystem, and Future Roadmap," *Applied System Innovation*. 2022. doi: 10.3390/asi5030057.

[3] M. Maazouz, A. Toubal, B. Bengherbia, O. Houhou, and N. Batel, "FPGA implementation of a chaos-based image encryption algorithm," *J. King Saud Univ. - Comput. Inf. Sci.*, 2022, doi: 10.1016/j.jksuci.2021.12.022.

[4] U. Zia, M. McCartney, B. Scotney, J. Martinez, M. AbuTair, J. Memon, and A. Sajjad, "Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains," *Int. J. Inf. Secur.*, 2022, doi: 10.1007/s10207-022-00588-5.

[5] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Inf. Sci. (Ny).*, 2019, doi: 10.1016/j.ins.2018.12.048.

[6] G. Veena and M. Ramakrishna, "A Survey on Image Encryption using Chaos-based Techniques," *Int. J. Adv. Comput. Sci. Appl.*, 2021, doi: 10.14569/IJACSA.2021.0120145.

[7] Z. Hua, Z. Zhu, S. Yi, Z. Zhang, and H. Huang, "Cross-plane colour image encryption using a two-dimensional logistic tent modular map," *Inf. Sci. (Ny).*, 2021, doi: 10.1016/j.ins.2020.09.032.

[8] Q. Lu, C. Zhu, and X. Deng, "An Efficient Image Encryption Scheme Based on the LSS Chaotic Map and Single S-Box," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.2970806.

[9] J. Arif, M. A. Khan, B. Ghaleb, J. Ahmad, A. Munir, U. Rashid, and A. Y. Al-Dubai, "A Novel Chaotic Permutation-Substitution Image Encryption Scheme Based on Logistic Map and Random Substitution," *IEEE Access*, 2022, doi: 10.1109/ACCESS.2022.3146792.

[10] S. Dhall, S. K. Pal, and K. Sharma, "A chaos-based probabilistic block cipher for image encryption," *J. King Saud Univ. - Comput. Inf. Sci.*, 2022, doi: 10.1016/j.jksuci.2018.09.015.

[11] A. A. Abdallah and A. K. Farhan, "A New Image Encryption Algorithm Based on Multi Chaotic System," *Iraqi J. Sci.*, 2022, doi: 10.24996/ijs.2022.63.1.31.

[12] K. M. Hosny, S. T. Kamal, M. M. Darwish, and G. A. Papakostas, "New image encryption algorithm using hyperchaotic system and fibonacci q-matrix," *Electron.*, 2021, doi: 10.3390/electronics10091066.

[13] Q. X. Huang, W. L. Yap, M. Y. Chiu, and H. M. Sun, "Privacy-Preserving Deep Learning With Learnable Image Encryption on Medical Images," *IEEE Access*, 2022, doi: 10.1109/ACCESS.2022.3185206.

[14] T. S. Ali and R. Ali, "A novel color image encryption scheme based on a new dynamic compound chaotic map and S-box," *Multimed. Tools Appl.*, 2022, doi: 10.1007/s11042-022-12268-6.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104211 |

[15] A. Kanso, M. Ghebleh, and M. B. Khuzam, "A Probabilistic Chaotic Image Encryption Scheme," *Mathematics*, 2022, doi: 10.3390/math10111910.

[16] Y. Dong, X. Huang, Q. Mei, and Y. Gan, "Self-Adaptive Image Encryption Algorithm Based on Quantum Logistic Map," *Secur. Commun. Networks*, 2021, doi: 10.1155/2021/6674948.

[17] R. Han, "A Hash-Based Fast Image Encryption Algorithm," *Wirel. Commun. Mob. Comput.*, 2022, doi: 10.1155/2022/3173995.

BIOGRAPHY

Shakuntala Bindiya is currently pursuing her M.Tech degree in Computer Science and Engineering from Raipur Institute Of Technology affiliated to Chhattisgarh Swami Vivekanand Technical University, Bhilai, Chhattisgarh, India. She has completed Diploma in Computer Science and Engineering from Government girls polytechnic, Bilaspur in 2012. She completed Bachelor of Engineering (B.E.) in Computer Science and Engineering fromGovernment Engineering College Bilaspur in 2015. Her research interest fields are Data Security, Image Processing, and Artificial Intelligence.

Vivek Kumar Sinha is currently working as an Assistant Professor in the Computer Science and Engineering Department at Raipur Institute of Technology, affiliated to Chhattisgarh Swami Vivekanand Technical University, Bhilai, Chhattisgarh, India. He is having 14 years of experience in teaching. He is currently Research Scholar at Lovely Professional University Phagwara, Jalandhar, Punjab, India. He has published 21 research papers in SCI, Scopus and other reputed journals and conferences.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details